Policies, Standards, and Exceptions Update

Presented to the ITB

August 6, 2009

Warren Dupuis

Policies Published

- Statewide Policy: Essential Information Security Roles
  - Purpose: This policy establishes the requirements to implement a computer security program based upon National Institute of Standards and Technology (NIST) guidance, specifically using the NIST risk management framework.
  - Policy Statement: It is the policy of the state of Montana that agencies implement an Information System Security Program as outlined in National Institute Standards and Technology Special Publications 800-100, Revision 2 (NIST SP800-100) Information Security Handbook: A Guide for Managers, utilizing the Risk Management Framework outlined in National Institute Standards and Technology Special Publication 800-39 (NIST SP800-39) Managing Risk From Information Systems.
  - Published: February 17, 2009 Effective: October 1, 2009

Policies Published (cont.)

- Statewide Policy: Computer Incident Management

  - Purpose: This policy establishes the requirements to implement a computer security incident management standard, plan, and associated procedures statewide.

  - Policy Statement: It is the policy of the state of Montana that agencies shall develop and implement an incident management program based on the National Institute of Standards and Technology Computer Incident Handling Guidance and the state of Montana Continuity of Government (COG) plans, policies, standards, and procedures for incident response.

  - Published: February 17, 2009 Effective: September 1, 2010

Policies Published (cont.)

- Statewide Policy: *Interim* Information Technology Project Management Policy
  - Purpose: This policy establishes the requirements for the utilization of project management methodologies as defined by the State of Montana Information Technology Project Management Office.
  - Policy Statement: State agencies must develop information technology resources in an organized, deliberative, and cost-effective manner. §2-17-505(2), MCA. State agencies shall implement best practice IT Project management methodologies to minimize unwarranted duplication and to ensure that similar information technology systems and data management applications are implemented and managed in a coordinated manner.
  - Published: March 3, 2009 Effective March 9, 2009 (*in revision*)

Policies in Development

- Enterprise Policy: Information Security Authorization: This policy establishes the requirement to implement Information Security (IS) Authorization processes and actions within agencies.

- Enterprise Policy: Information Systems Identification and Authentication - This policy establishes the requirement to implement Information Security Identification and Authentication standard(s) and associated procedures within agencies.

- Enterprise Policy: Configuration Management - This policy establishes the requirement to implement Information Security Configuration Management standard(s) and associated procedures within agencies.

Policies in Development

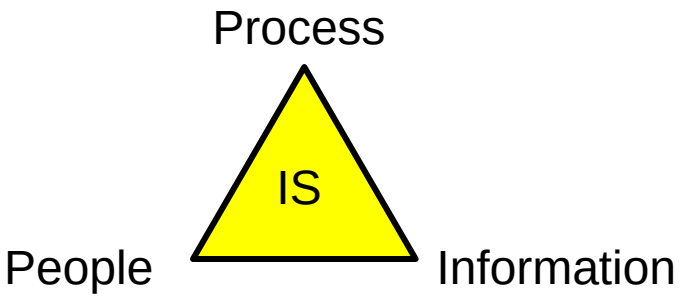
- Enterprise Policy: Information Systems Risk Assessment - This policy establishes the requirement to implement information security (IS) risk assessment processes and actions within agencies.

- Enterprise Policy: Information Security Systems and Communications Protection - This policy establishes the requirement to implement System and Communication Protection processes and actions within agencies.

- Enterprise Policy: Information Security Contingency Planning - This policy establishes the requirement to implement Information Security Contingency Planning processes and actions within agencies.

Policies in Development (cont.)

- Enterprise Policy: Information Security Awareness and Training - This policy establishes the requirement to implement Information Security Awareness and Training programs, processes and actions within agencies.



The focus is on the business managing risks to the information system!

Standards in Development

- Enterprise Standard: Secured eGovernment Service Access - This Standard establishes the specifications and requirements for agencies to implement a federated single sign-on, or point-of-entry, for all eGovernment services using the state's SummitNet network. - Posted for Public Comment

- Enterprise Standard: Electronic Payment Processing Portal - This Standard establishes the specifications and requirements for the single portal, or point-of-entry, for all online electronic payment processing. - Posted for Public Comment

Exceptions

- The Department of Administration requested an enterprise exception to the Usernames and Passwords policy (ENT-SEC-063) for the ePass application.
  - CIO approved this request. (4/7/2009)

CIO Advisories

- The CIO Approved the limited use of Open Office software as a non-supported product. (January 28, 2009)

- The CIO approved MPEG-4 and H.264 as the technical standards for all streaming media, both video and audio. (April 9, 2009)

- Statewide Policy: Internet and Intranet Security (ENT-SEC-012) has been changed to reflect organizational changes in the Information Technology Services Division. Responsibility for performing "standard security check" for web servers referenced under paragraph VI.B, are now the responsibility of individual agencies. (June 5, 2009)

Questions?